Cisco Identity Services Engine の証明書更新に関する設定ガイド

目次

概要

このドキュメントでは、Cisco Identity Services Engine（ISE）で証明書を更新するためのベストプラクティスと事前措置について説明します。 また、証明書の期限切れなどのこれから起きるイベントを管理者に警告するためのアラームと通知のセットアップ方法も確認します。

> **注:** このドキュメントは、証明書のトラブルシューティング ガイドではありません。

前提条件

要件

次の項目に関する知識が推奨されます。

- X509 証明書
- Cisco ISE と証明書の設定

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco ISE リリース 1.2.0.899
- アプライアンスまたは VMware

背景説明

ISE 管理者は、いつかは ISE 証明書が期限切れになるという事態に遭遇します。 ISE サーバ上の証明書が期限切れになり、新しい有効な証明書と交換しなかった場合は、深刻な問題が発生します。

> **注:** 拡張認証プロトコル（EAP）に使用されている証明書が期限切れになると、クライアントが ISE 証明書を信頼しなくなるため、認証が一切できなくなります。 HTTPS プロトコル証明書が期限切れになると、リスクがさらに高まります。 管理者は ISE にログインできなくなり、分散導入が機能しなくなり、複製が停止します。

この例では、1 か月以内に期限が切れる証明書が認証局（CA）サーバから ISE にインストールされています。 ISE 管理者は、古い証明書が期限切れになる前に新しい有効な証明書を ISE にインストールする必要があります。 この事前のアプローチによって、ダウンタイムが阻止または最小限に抑えられ、エンドユーザーへの影響が回避されます。 新しくインストールした証明書の期間が始まったら、新しい証明書で EAP または HTTPS プロトコルを有効にすることができます。

古い証明書が期限切れになる前にアラームを発生させ、新しい証明書のインストールを管理者に通知するように ISE を設定できます。

> **注:** このドキュメントでは、証明書の更新の影響を示すために HTTPS と自己署名証明書を使用しますが、このアプローチは実稼働システムに適用しないでください。 EAP プロトコルと HTTPS プロトコルの両方に対して 1 つの CA 証明書を使用することをお勧めします。

設定

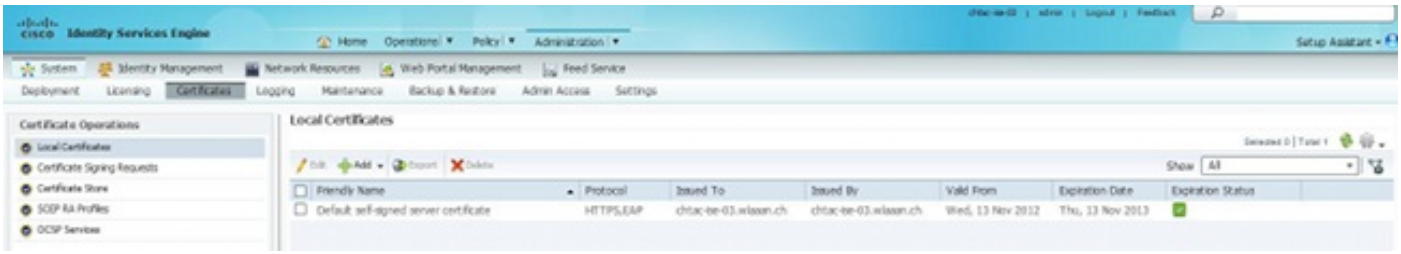
ISE 自己署名証明書の表示

ISE をインストールすると、自己署名証明書が生成されます。 自己署名証明書は、管理アクセスや分散導入（HTTPS）内部の通信だけでなく、ユーザ認証（EAP）にも使用されます。 実稼働システムでは、自己署名証明書ではなく CA 証明書を使用してください。

> **ヒント**： 追加情報については、『Cisco Identity Services Engine Hardware Installation Guide, Release 1.2 』の「Certificate Management in Cisco ISE 」の項を参照してください。

ISE 証明書の形式は、プライバシー強化メール（PEM）または Distinguished Encoding Rules（DER）にする必要があります。

初期自己署名証明書を確認するには、ISE コンソールで、[Administration] > [System] > [Certificates] > [Local Certificates] に移動します。



サーバ証明書を証明書署名要求（CSR）を介して ISE にインストールし、HTTPS または EAP プロトコル用の証明書を変更したら、自己署名サーバ証明書はそのまま残りますが、使用されなくなります。

> **注意**： HTTPS プロトコルのための変更には ISE サービスを再起動する必要があるため、数分間のダウンタイムが発生します。 EAP プロトコルの変更は、ISE サービスの再起動がトリガーされず、ダウンタイムが発生しません。

証明書を変更する時期の特定

インストールされた証明書がもうすぐ期限切れになるとします。 証明書が期限切れになってから更新するのと、証明書が期限切れになる前に変更するのとどちらが適切だと思いますか。 証明書の切り替えを計画し、切り替えによるダウンタイムに対処する時間を持てるように、証明書は期限切れになる前に変更すべきです。

証明書はいつ変更すべきでしょうか。 開始日が古い証明書の失効日より前である新しい証明書を取得します。 この 2 つの日付の間の期間が移行期間です。

> **注意**： HTTPS を有効にすると、ISE サーバ上のサービスが再起動されるため、数分間のダウンタイムが発生します。

この画像は、CA から発行され、2013 年 11 年 29 日に期限切れになる証明書に関する情報を示しています。

証明書署名要求の生成

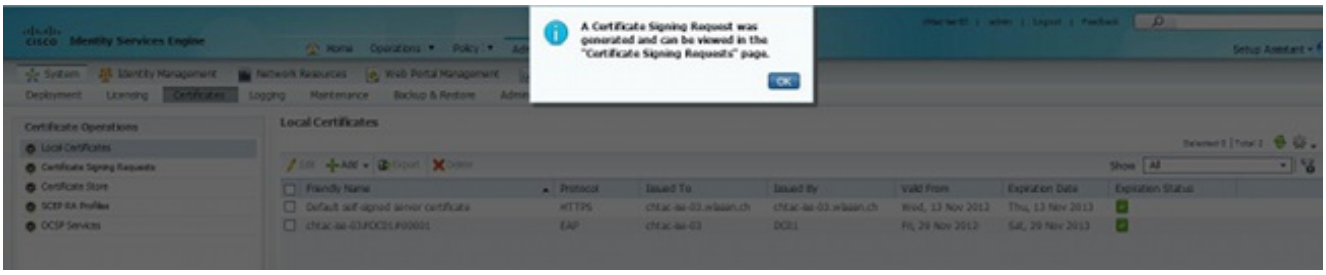
次の手順では、CSR を介して証明書を更新する方法を説明します。

1. ISE コンソールで、[Add] > [Generate Certificate Signing Request] に移動します。

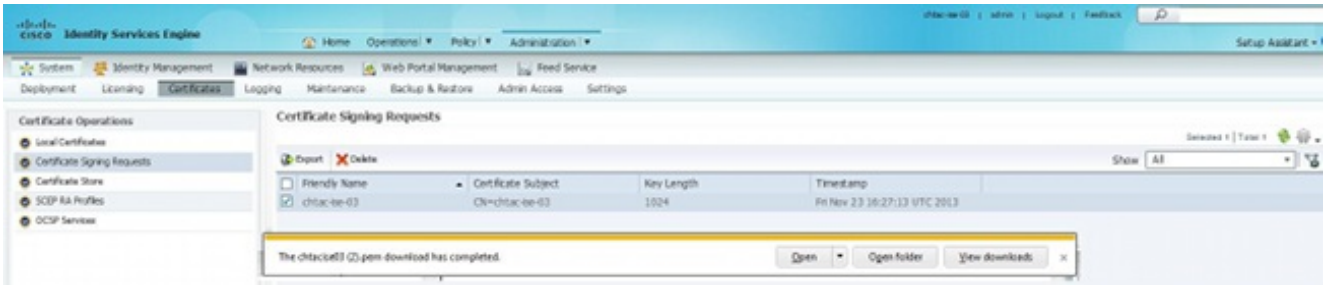
2. [Certificate Subject] テキスト フィールドに入力する必要がある最小限の情報は CN=ISEfqdn です。ここで、*ISEfqdn* は ISE の完全修飾ドメイン名（FQDN）です。 O（組織）、OU（組織単位）、C（国）などのフィールドをカンマで区切って [Certificate Subject] に追加します。

3. [Subject Alternative Name (SAN)] テキスト フィールド行の 1 つで、ISE FQDN を繰り返す必要があります。 代行名またはワイルドカード証明書を使用する場合、2 つ目の SAN フィールドを追加できます。

4. ポップアップ ウィンドウに CSR フィールドが正しく入力されたかどうかが示されます。



5. CSR をエクスポートするために、左側のパネルで [Certificate Signing Requests] をクリックし、CSR を選択し、[Export] をクリックします。

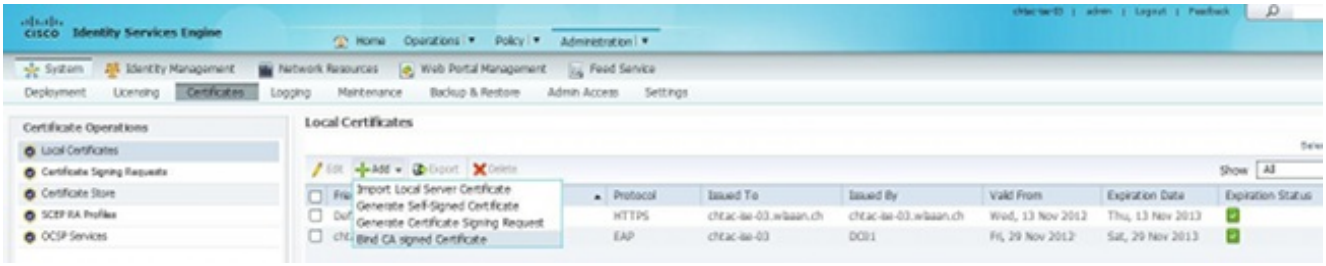


6. CSR がコンピュータ上に保存されます。 それを署名用に CA に送信します。

証明書のインストール

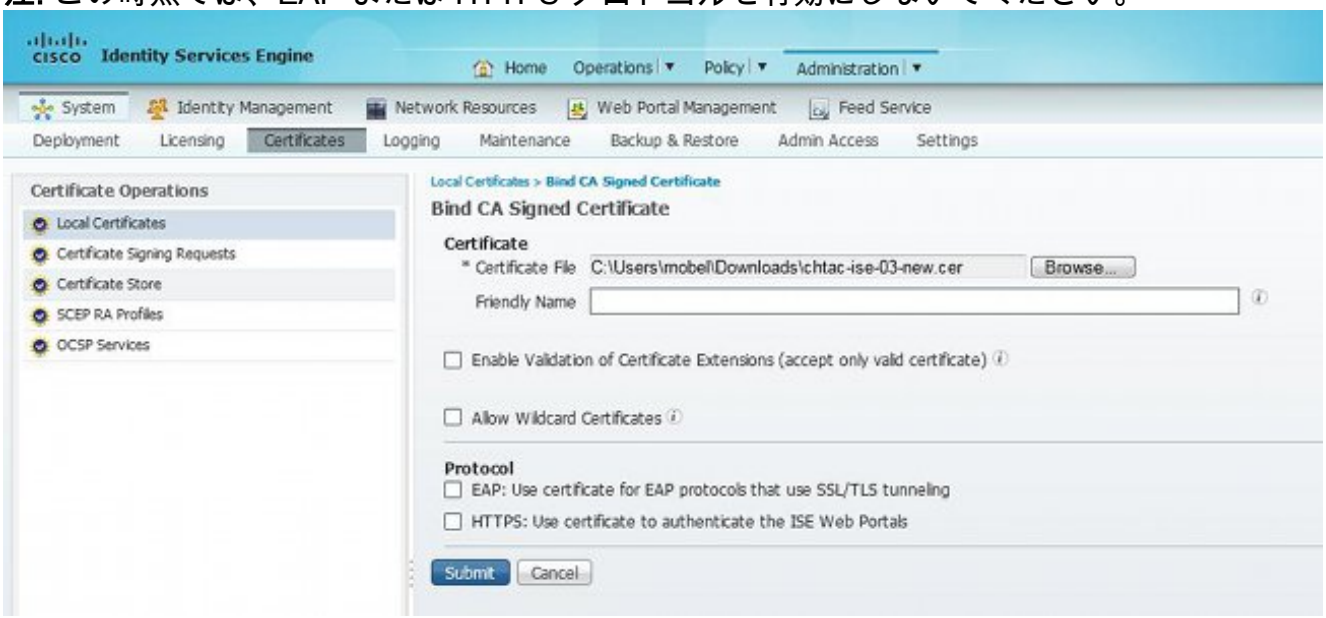
CA から最終的な証明書を受信したら、その証明書を ISE に追加する必要があります。

1. ISE コンソールの左側のパネルで [Local Certificates] をクリックしてから、[Add] と [Bind CA signed Certificate] をクリックします。

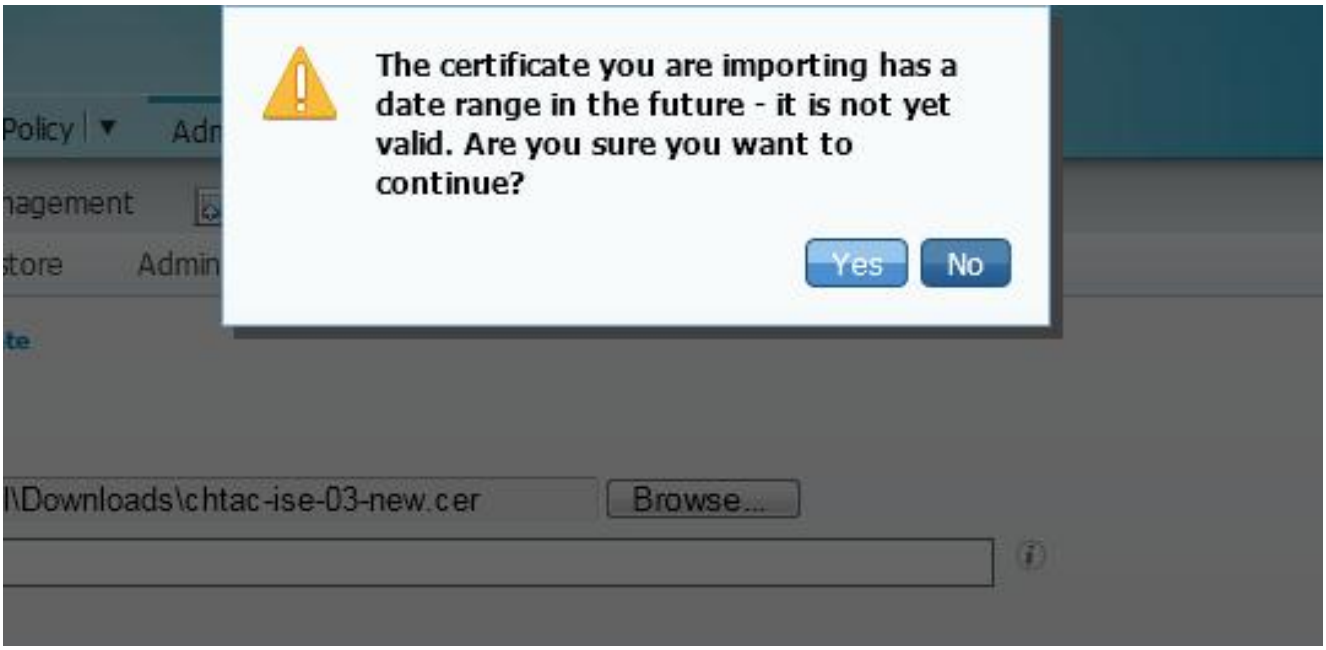


2. [Friendly Name] テキスト フィールドに証明書の簡潔でわかりやすい説明を入力します。

   注: この時点では、EAP または HTTPS プロトコルを有効にしないでください。

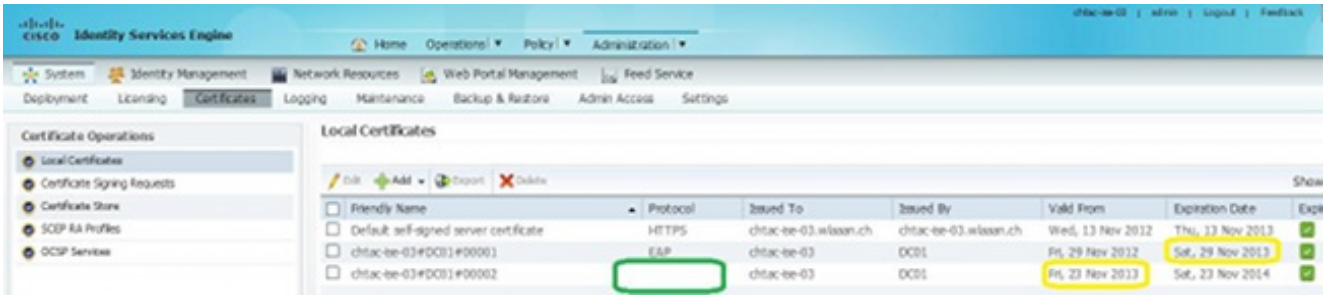


3. 古い証明書が期限切れになる前に新しい証明書をインストールしているため、有効期限（この例では 2013 年 11 月 23 日）に関するエラーが表示されます。



4. 続行するには [Yes] をクリックします。 緑色で強調表示されているように、これで証明書はインストールされましたが、使用中にはなっていません。 失効日と発効日の重複が黄色で

強調表示されています。



注: 分散導入で自己署名証明書を使用する場合は、プライマリ自己署名証明書をセカンダリ ISE サーバの信頼できる証明書ストアにインストールする必要があります。 同様に、セカンダリ自己署名証明書をプライマリ ISE サーバの信頼できる証明書ストアにインストールする必要があります。 これにより、ISE サーバは相互に認証できます。 そうしなかった場合は、導入が中断する可能性があります。 サードパーティ CA から証明書を更新する場合は、ルート証明書チェーンが変更されているかどうかを確認し、それに応じて ISE 内の信頼できる証明書ストアを更新します。 両方のシナリオにおいて、ISE ノード、エンドポイントのオペレーティング システム、およびサプリカントがルート証明書チェーンを検証可能なことを確認します。

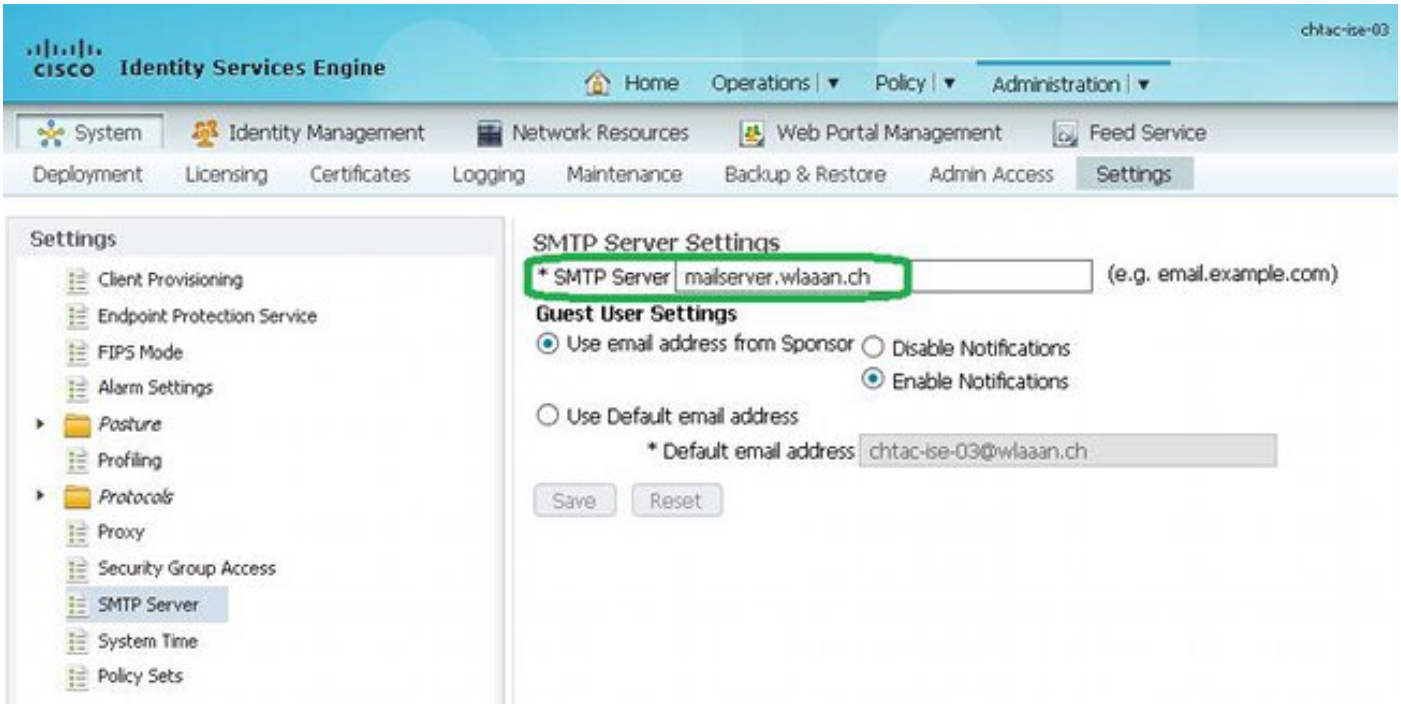
警告システムの設定

Cisco ISE は口ーカル証明書の失効日が 90 日以内に迫ったときに通知します。 このような事前通知により、証明書の期限切れを回避して、証明書の更新を計画し、ダウンタイムを阻止または最小限に抑えることができます。

この通知はいくつかの方法で表示されます。

- 色付きの期限切れステータス アイコンが、[Local Certificates] ページに表示されます。
- 期限切れメッセージが Cisco ISE システム診断レポートに表示されます。
- 期限切れアラームは、期限切れの 90 日前と 60 日前に生成されたあと、期限切れ前の 30 日間は毎日生成されます。

期限切れアラームの電子メール通知を行うように ISE を設定します。 ISE コンソールで、[Administration] > [System] > [Settings] > [SMTP Server] に移動して、Simple Mail Transfer Protocol (SMTP) サーバを特定し、アラームの電子メール通知が送信されるようにその他のサーバ設定を定義します。

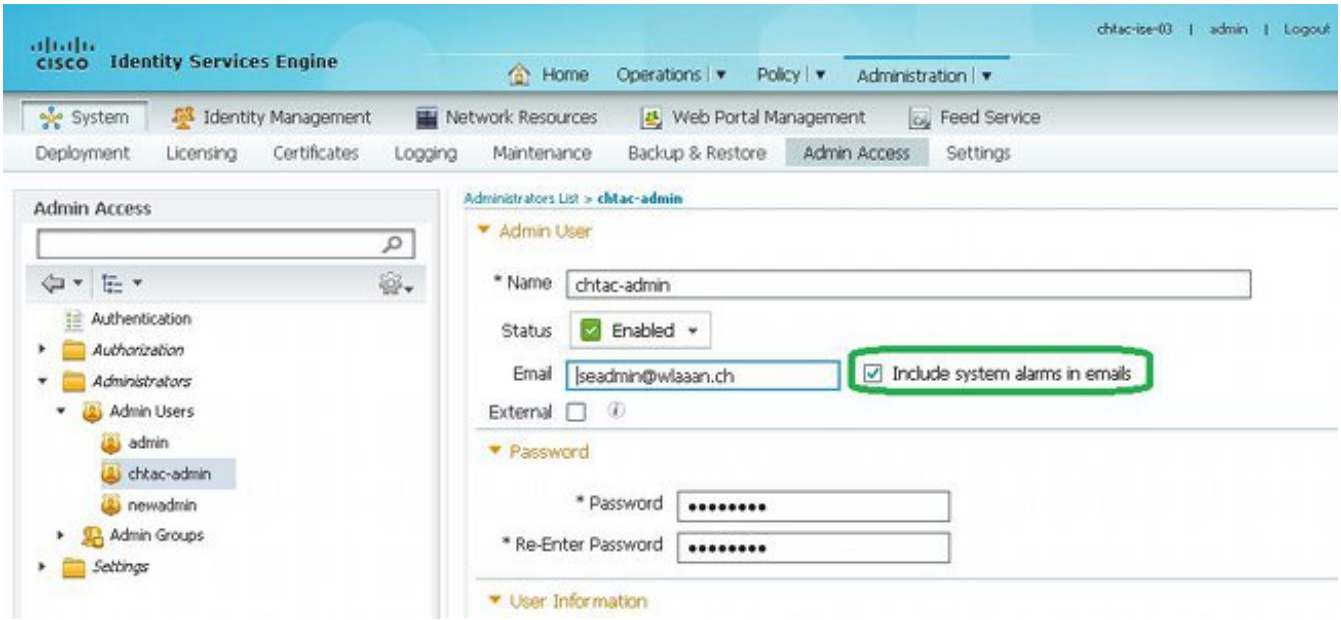


通知をセットアップするには、次の 2 つの方法があります。

- 管理者に通知するには、管理者アクセスを使用します。

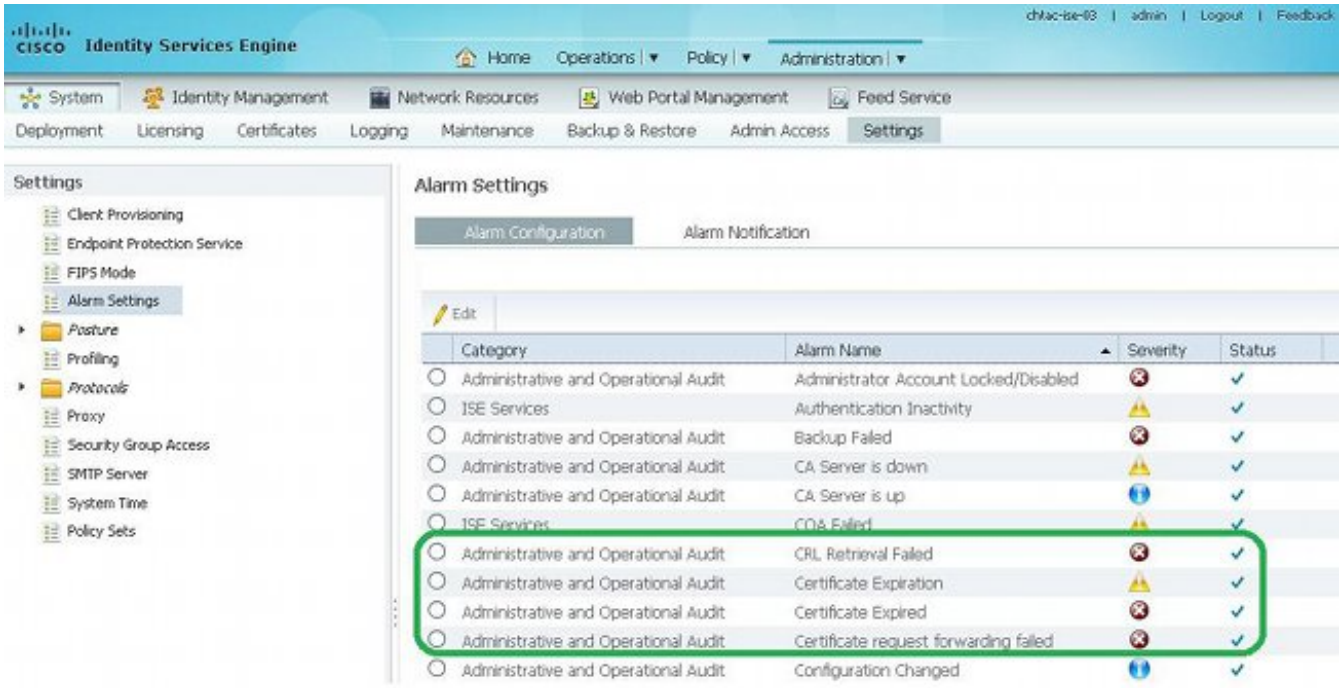
  [Administration] > [System] > **[Admin Access] > [Administrators] > [Admin Users] に移動します。**

  アラーム通知を受信する必要のある管理者ユーザの [Include system alarms in emails] チェックボックスをオンにします。 アラーム通知の送信者の電子メール アドレスは ise@*hostname* としてハードコードされています。

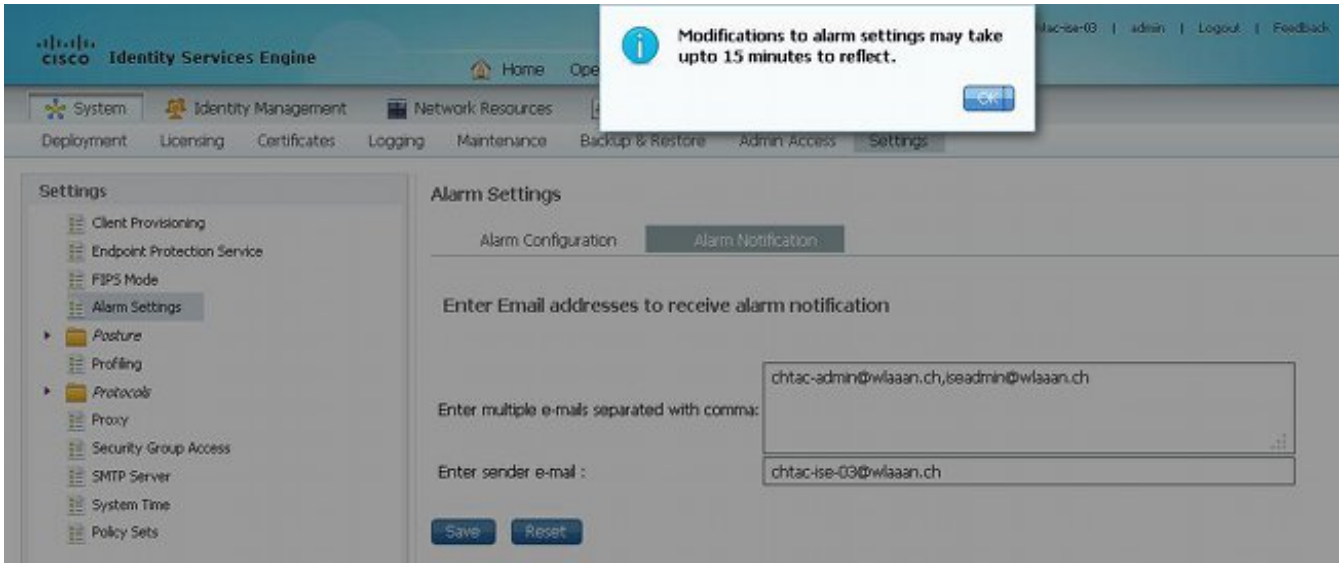


- ユーザに通知するには、ISE アラーム設定を構成します。

  [Administration] > [System] > [Settings] > [Alarm Settings] > [Alarm Configuration] に移動します。



注: アラームを発生させたくないカテゴリのステータスを無効にします。[Alarm Notification] をクリックして、通知対象のユーザの電子メール アドレスを入力し、設定の変更を保存します。 変更が有効になるまで最大 15 分かかります。

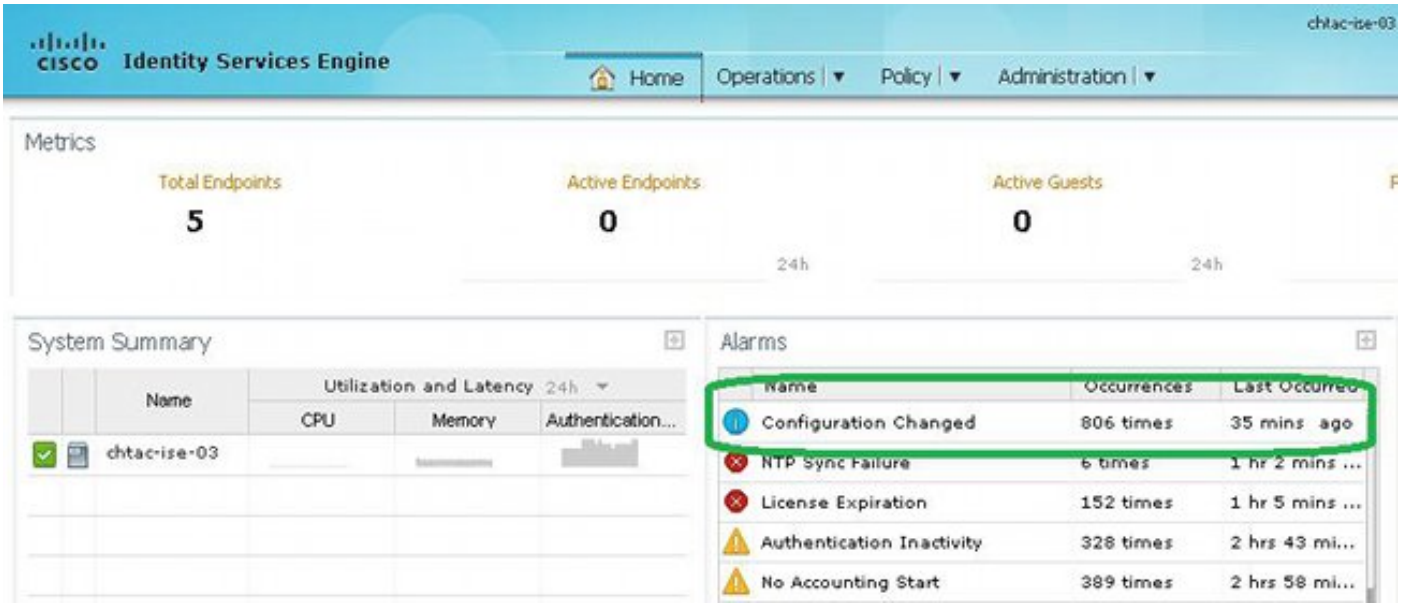


確認

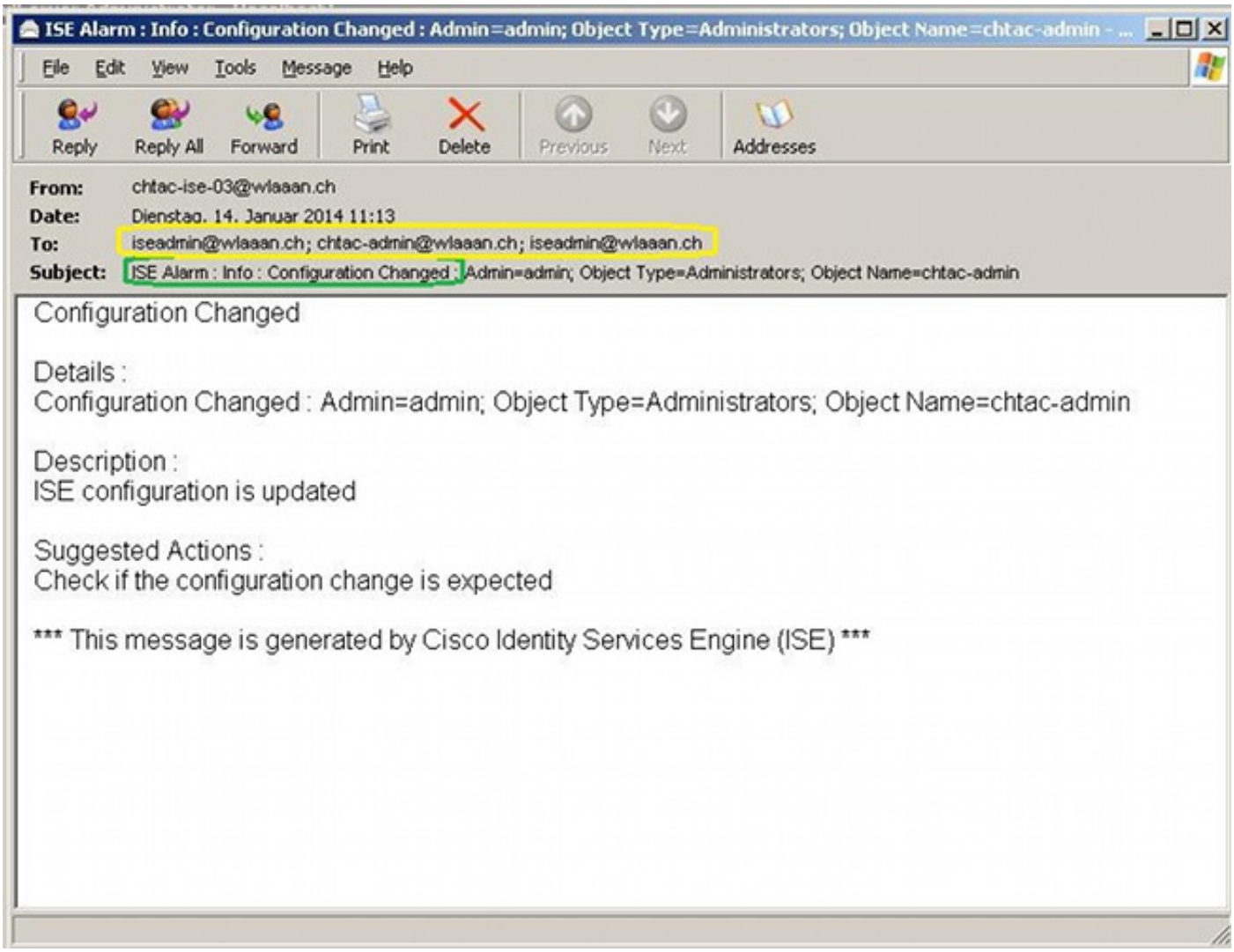
このセクションでは、設定が正常に機能していることを確認します。

警告システムの確認

警告システムが正しく機能していることを確認します。 この例では、設定の変更によって、情報の重大度を含むアラートが生成されます（情報アラームが最も低い重大度ですが、証明書の期限切れはそれよりも高い重大度である警告を生成します）。



ISE から送信される電子メール アラームの例を以下に示します。



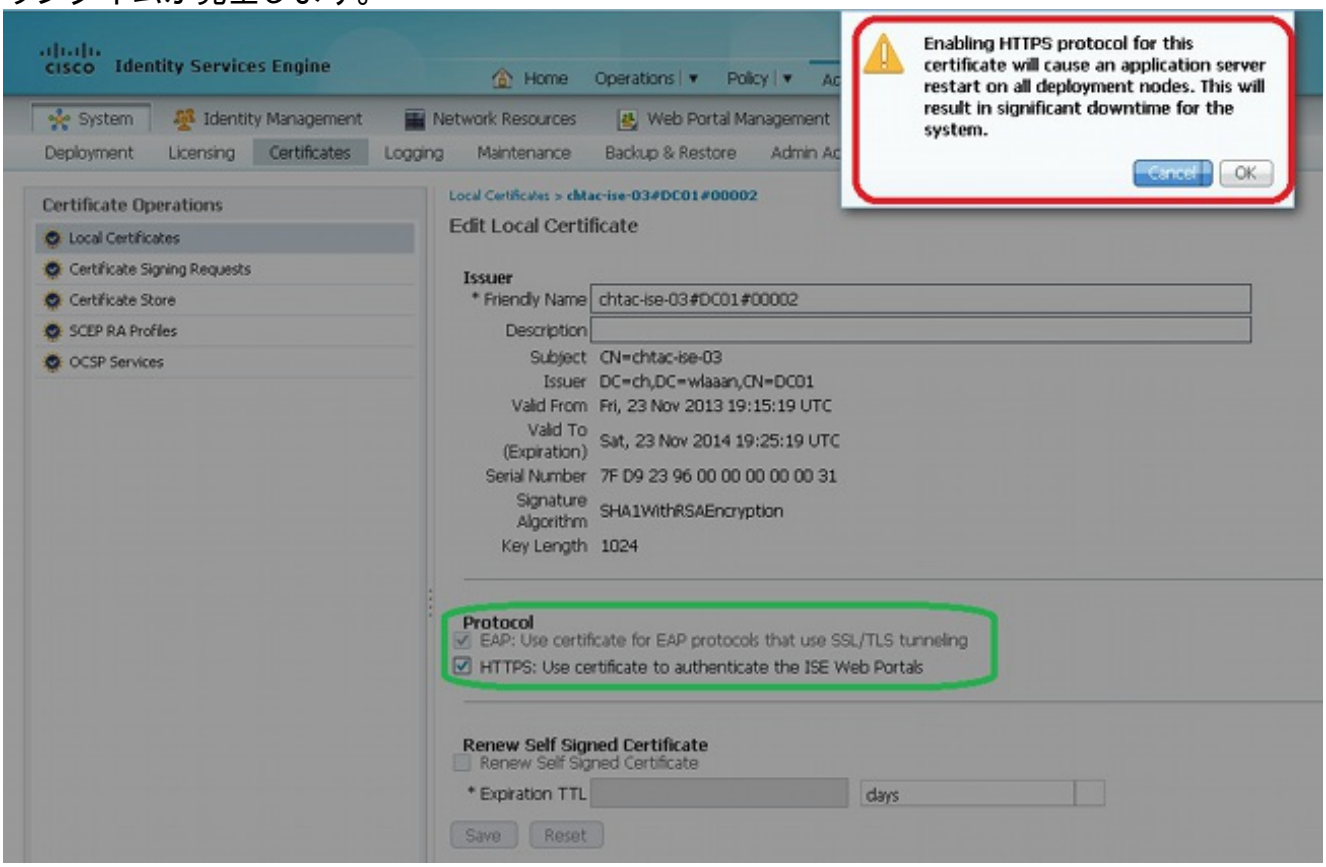
注: 黄色で強調表示されているように、この例では、ISE が iseadmin@wlaaan.ch に電子メール アラーム メッセージを 2 回送信しています。 この電子メール アドレスは、「警告システムの設定」で説明した両方の方法による通知を受信するようにセットアップされています。

証明書変更の確認

この手順では、証明書が正しくインストールされていることを確認する方法とプロトコルを EAP または HTTPS 用に変更する方法について説明します。

1. ISE コンソールで、[Administration] > [Certificates] > [Local Certificates] に移動し、新しい証明書を選択して詳細を表示します。

   注意： HTTPS プロトコルを有効にすると、ISE サービスが再起動されるため、サーバのダウンタイムが発生します。



   この例では、HTTPS が ISE サービスを再起動するとします。

2. ISE サーバ上の証明書ステータスを確認するために、次のコマンドを CLI に入力します。

```
CLI:> show application status ise
```

3. すべてのサービスがアクティブになったら、管理者としてログインします。

4. 分散導入シナリオの場合は、ISE コンソールで [Administration] > [System] > [Deployment] > [Node Status] に移動して、ノード ステータスを確認します。

5. エンド ユーザ認証が成功することを確認します。 ISE コンソールで [Operations] > [Authentications] に移動して、Protected Extensible Authentication Protocol（PEAP）/EAP-Transport Layer Security（TLS）認証用の証明書を確認します。

証明書の確認

証明書を外部からチェックする場合は、組み込みの Microsoft Windows ツールまたは OpenSSL ツールキットを使用します。

OpenSSL はセキュア ソケット レイヤ (SSL) プロトコルのオープン ソース実装です。 証明書で独自のプライベート CA が使用されている場合は、ローカル マシンにルート CA 証明書を配置して、OpenSSL オプション *-CApath* を使用する必要があります。 中間 CA が存在する場合は、それも同じディレクトリに配置する必要があります。

証明書に関する一般情報を取得してそれを検証するには、以下を使用します。

```
openssl x509 -in certificate.pem -noout -text
openssl verify certificate.pem
```

また、OpenSSL ツールキットで証明書を変換する方が便利な場合があります。

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

結論

新しい証明書は ISE にインストールしてからアクティブにすることができるため、古い証明書が期限切れになる前に新しい証明書をインストールすることをお勧めします。 古い証明書の失効日と新しい証明書の開始日の間の重複期間が、証明書を更新してそれらのインストールを最小限のダウンタイムでまたはダウンタイムなしで計画するための時間になります。 新しい証明書の有効期間が始まったら、EAP または HTTPS プロトコル (またはその両方) を有効にします。
HTTPS を有効にした場合は、サービスが再起動されることに注意してください。